Claims

What is claimed is:

1. A universal password generator for generating a password in response to a challenge from a compatible challenging system, the universal password generator comprising:

a) an input transducer for receiving a challenge, the challenge provided by the compatible challenging system to an individual and for being provided to the input transducer by the individual;

b) a memory for storing secure data, the secure data for use in performing a predictable secure process wherein absent knowledge of the secure data, the secure process is not capable of being performed;

c) a secure processor for securely processing the received challenge using the secure process and the stored secure data to determine a response compatible with the challenging system thereto, the challenge being securely processed such that the individual is not able to determine a same response to a same challenge absent the universal password generator; and,

d) a display for displaying the response in a human intelligible form,

wherein, in use, upon providing a challenge to the input transducer, the response is displayed which, when entered manually into the compatible challenging system, provides access thereto.

2. A universal password generator according to claim 1, wherein the secure data comprises an encrypting key.

3. A universal password generator according to claim 1, wherein the secure data comprises data indicative of instructions for execution as a secure process.

4. A universal password generator according to claim 1, comprising a clock for providing a time value for use in secure processing of the challenge in dependence upon the time value, wherein in use, the response is different for different time values.

5. A universal password generator according to claim 1, comprising a security input device for authenticating the individual.

6. A universal password generator according to claim 5, wherein the security input device is a biometric imager for capturing an image of a biometric information source.

7. A universal password generator according to claim 6, wherein the security input device comprises a processor for processing the image, for comparing data derived from the image with a stored template, and for, in dependence upon a comparison result, authenticating the individual.

8. A universal password generator according to claim 3, wherein the secure process comprises a plurality of secure processes, each secure process from the plurality of secure processes being associated with a compatible challenging system.

9. A universal password generator according to claim 8, comprising a second secure processor for identifying the compatible challenging system in accordance with the provided challenge, the second secure processor for selecting a secure process from the plurality of secure processes and for securely processing the received challenge.

10. A universal password generator according to claim 9, wherein the secure processor and the second secure processor are same.

11. A method for generating passwords using a universal password generator in response to a challenge from a compatible challenging system, the method comprising the steps of:

a) receiving a challenge provided by the challenging system;

b) securely processing the received challenge according to securely stored data;

c) determining a response in dependence upon the secure processing, the response compatible with the challenging system such that an individual is not able to determine a same response to a same challenge absent the universal password generator; and,

d) displaying the response in an human intelligible form,

wherein upon providing the response to the challenging system access is provided thereto.

12. A method for generating passwords according to claim 11, wherein the step of securely processing comprises the step of encrypting the challenge according to the secure data stored, wherein the secure data comprises an encrypting key.

13. A universal password generator according to claim 11, wherein the step of securely processing the received challenge to determine a response comprises the step of providing a time value determined by a clock such that the response is different for different time values.

14. A method for generating passwords according to claim 11, wherein the step of securely processing the received challenge comprises the steps of:

a) identifying the challenging system in dependence upon the provided challenge; and,

b) selecting a secure process associated with the identified challenging system, the secure process being selected from a plurality of secure processes dependent on stored secure data.

15. A method for generating passwords according to claim 11, comprising prior to step (a) the step of authenticating an individual using a biometric sample provided to an input security device.

16. A method for generating passwords according to claim 15, comprising the step of:

e) providing a biometric information source to a biometric imager,

f) capturing an image of the biometric information source;

g) generating data derived from the imaged biometric information; and,

h) comparing the generated data with stored templates of biometric data, and for, in dependence upon a comparison result, performing one of authenticating and other than authenticating the individual,

wherein the step (d) is performed in dependence upon the result of the step (h).

17. A universal password generator for generating a password in response to a challenge from a compatible challenging system, the universal password generator comprising:

a) an input transducer for receiving a challenge, the challenge provided by the compatible challenging system to an individual and for being provided to the input transducer by the individual;

b) a memory for storing secure data;

c) a secure processor for securely processing the received challenge using stored secure data to determine a response compatible with the challenging system and requiring the stored secure data for determination thereof; and,

d) a display for displaying the response in a human intelligible form,

wherein, in use, upon providing a challenge to the input transducer, the response is displayed which, when entered manually into the compatible challenging system, provides access thereto.